Information Security Principles

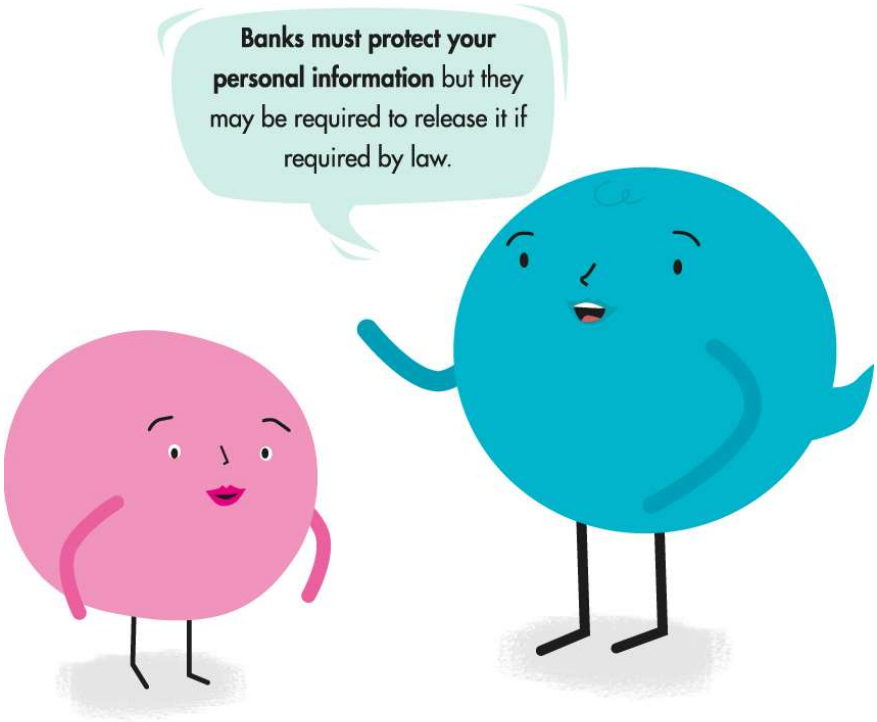
Dr. Bhaskar Mondal

CIA

- ***Confidentiality*** – restrict access by unauthorized individuals
- ***Integrity*** – data has not been altered in an unauthorized manner
- ***Availability*** – information can be accessed and modified by authorized individuals in an appropriate timeframe

Confidentiality

- "Need to know" basis for data access
  - How do we know who needs what data?
    Approach: access control specifies *who* can access *what*
  - How do we know a user is the person she claims to be?
    Need her identity and need to verify this identity
    Approach: identification and authentication
- Analogously: "Need to access/use" basis for physical assets
  - E.g., access to a computer room, use of a desktop
- Confidentiality is:
  - difficult to ensure
  - easiest to assess in terms of success (binary in nature: Yes / No)



- Integrity is Concerned with unauthorized modification of assets (= resources)
- Confidentiality: concerned with access to assets

Integrity (Integrity vs. Confidentiality)

- Integrity is more difficult to *measure* than confidentiality

  Not binary but *degrees of integrity*

  Context-dependent - means different things in different contexts

  Could mean *any subset of* these asset properties:

  { precision / accuracy / currency / consistency /

  meaningfulness / usefulness / ...}

- Types of integrity—an example
  - Quote from a politician
  - Preserve the quote (data integrity) but misattribute (origin integrity)

Availability (1)

"*Full implementation of availability is security's next challenge*"

E.g. Full implemenation of availability for Internet users (with ensuring security)

- Complex
  - Context-dependent

    Could mean *any subset of* these asset (data or service) properties :

    { usefulness / sufficient capacity / progressing at a proper pace / completed in an acceptable period of time / ...}

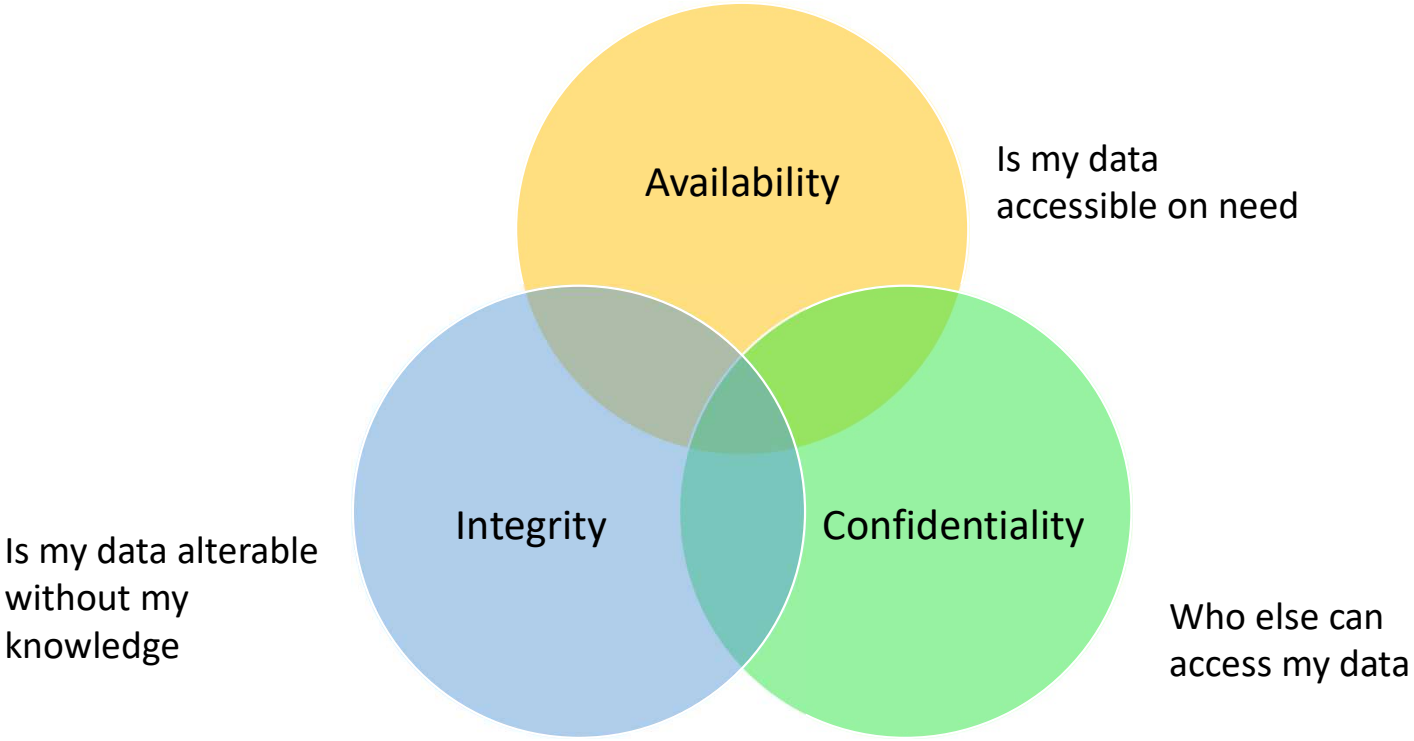
[Pfleeger & Pfleeger]

We can say that an asset (resource) is available if

- Timely request response
- Fair allocation of resources (no starvation!)
- Fault tolerant (no total breakdown)
- Easy to use in the intended way
- Provides controlled concurrency (concurrency control, deadlock control, ...)

[Pfleeger & Pfleeger]

CIA Principle



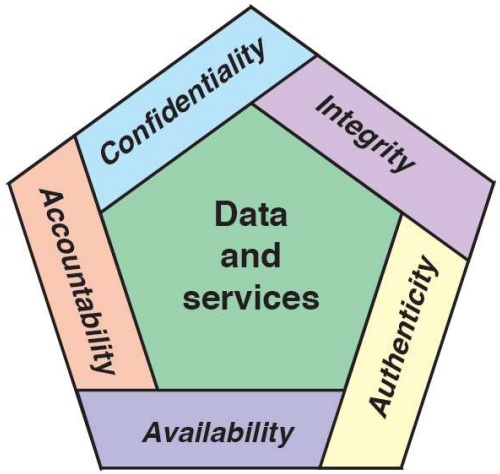
Need to Balance CIA

- Example 1: C vs. I+A
  - Disconnect computer from Internet to increase confidentiality
  - Availability suffers, integrity suffers due to lost updates
- Example 2: I vs. C+A
  - Have extensive data checks by different people/systems to increase integrity
  - Confidentiality suffers as more people see data; availability suffers due to locks on data under verification)

CIA or CIAAAN

(other security components added to CIA)

- Authentication
- Authorization
- Non-repudiation/ Accountability



Additional concepts:

Authenticity	Verifying that users are who they say they are and that each input arriving at the system came from a trusted source
Non-repudiation/ Accountability	Being able to trace the responsible party/process/entity in case of a security incident or action.

Security Services (X.800)

Authentication	Access Control	Data Confidentiality	Data Integrity	Non-Repudiation
• assurance that the communicating entity is the one it claims to be • peer entity authentication: mutual confidence in the identities of the parties involved in a connection • Data-origin authentication: assurance about the source of the received data	• The prevention of unauthorized use of a resource • who can have access to a resource, • under what conditions access can occur, • what those accessing the resource are allowed to do	• protection of data from unauthorized disclosure (against eavesdropping) • traffic flow confidentiality (anonymous) is one step ahead	• assurance that data received are exactly as sent by an authorized sender • i.e. no modification, insertion, deletion, or replay	• protection against denial by one of the parties in a communication • Origin non-repudiation • Destination non-repudiation

Relationships among integrity, data-origin authentication and non-repudiation